UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/740,411	12/19/2000	Chin-Long Chen	POU920000117US1	3694

7590 01/11/2005

Lawrence D. Cutter, Attorney
IBM Corporation, Intellectual Property Law Dept.
2455 South Rd., M/S P386
Poughkeepsie, NY 12601

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/740,411	CHEN ET AL.	
	Examiner	Art Unit	
	Aravind K Moorthy	2131	

-- Th MAILING DATE of this communication appears on the cover sheet with the correspond nc address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-10 are pending in the application.

2. Claims 1-10 stand being rejected.

Response to Amendment

3. The examiner approves the amendments made to the specification.

Response to Arguments

4. Applicant's arguments, see page 11, filed 9/9/04, with respect to claim rejections 35 USC § 101 have been fully considered and are persuasive. The rejection of claims 1-10 has been withdrawn.

5. Applicant's arguments, see pages 12-13, filed 9/9/04, with respect to the claim objection have been fully considered and are persuasive. The objection of claims 1, 6 and 7 has been withdrawn.

6. Applicant's arguments filed 9/9/04 been fully considered but they are not persuasive.

On page 14, the applicant argues that the cited patent is not directed to circuits for performing modular exponentiation operations.

The examiner respectfully disagrees. The scope of a product claim is defined by the apparatus's structures. Another apparatus with the same structures is presumably capable of performing the function of the claimed apparatus. Therefore the apparatus of the prior art anticipates the apparatus of the claimed invention. See MPEP 2106 2(c)

"Office personnel should begin claim analysis by identifying and evaluating each claim limitation. For processes, the claim limitations will define steps or acts to be performed. For products, the claim limitations will define discrete physical structures or materials. Product

claims are claims that are directed to either machines, manufactures or compositions of matter. The discrete physical structures or materials may be comprised of hardware or a combination of hardware and software."

2106 IV (B) 2(a)

"Products may be either machines, manufactures, or compositions of matter. A machine is "a concrete thing, consisting of parts or of certain devices and combinations of devices." Burr v. Duryee, 68 U.S. (1 Wall.) 531, 570 (1863)."

On page 15, the applicant argues that the cited patent does not appear to teach modulo N multiplication and that it does not teach structures, devices or methods for performing modulo N exponentiation operations.

The examiner respectfully disagrees. It is clearly shown in figure 3 that the cited patent does teach modulo N multiplication and the following figures that it is a structure, device and method for performing modulo N exponentiation operations.

On page 16, the applicant argues that the cited patent does not teach a circuit nor method for producing exponentiation modulo N results.

The examiner respectfully disagrees. The scope of a product claim is defined by the apparatus's structures. Another apparatus with the same structures is presumably capable of performing the function of the claimed apparatus. Therefore the apparatus of the prior art anticipates the apparatus of the claimed invention. See MPEP 2106 2(c)

"Office personnel should begin claim analysis by identifying and evaluating each claim limitation. For processes, the claim limitations will define steps or acts to be performed. For products, the claim limitations will define discrete physical structures or materials. Product

claims are claims that are directed to either machines, manufactures or compositions of matter. The discrete physical structures or materials may be comprised of hardware or a combination of hardware and software."

2106 IV (B) 2(a)

"Products may be either machines, manufactures, or compositions of matter. A machine is "a concrete thing, consisting of parts or of certain devices and combinations of devices." Burr v. Duryee, 68 U.S. (1 Wall.) 531, 570 (1863)."

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claim 6-10 are rejected under 35 U.S.C. 102(b) as being anticipated by Monier (USP 5,764,554).

As per claim 6 Monier teaches a circuit having two input operands for signals representing binary numbers (see figure 1), a first register for providing input operands to said circuit (figure 1, elements 16 and 17), second register means for storing output from said circuit (figure 1, element 18), and a means for controlling input operand selection to said circuit (figure 1, elements 23 and 24).

As per claim 7, Monier teaches a modular multiplication circuit having two inputs operands for signals representing binary numbers (see figure 1), a first multiplexor for selecting input signals for first input (figure 1, element 23), a second multiplexor for selecting input

signals for second input (figure 1, element 24) a first output register (figure 1, element 16), a second output register (figure 1, element 11), and selector circuit for supplying output to one or both of first and second registers (figure 1, elements 14 and 24), and means for controlling first and second multiplexors (figure 1, element 23).

The scope of a product claim is defined by the apparatus's structures. Another apparatus with the same structures is presumably capable of performing the function of the claimed apparatus. Therefore the apparatus of the prior art anticipates the apparatus of the claimed invention. See MPEP 2106 2(c)

"Office personnel should begin claim analysis by identifying and evaluating each claim limitation. For processes, the claim limitations will define steps or acts to be performed. For products, the claim limitations will define discrete physical structures or materials. Product claims are claims that are directed to either machines, manufactures or compositions of matter. The discrete physical structures or materials may be comprised of hardware or a combination of hardware and software."

2106 IV (B) 2(a)

"Products may be either machines, manufactures, or compositions of matter. A machine is "a concrete thing, consisting of parts or of certain devices and combinations of devices." Burr v. Duryee, 68 U.S. (1 Wall.) 531, 570 (1863)."

As per claim 8, Monier teaches a finite state machine which switches states in dependence on the values of e; and a counter (column 5, lines 47-55).

As per claim 9, Monier teaches said counter counts from 0 to t (column 16, lines 53-57 and column 1, lines 59-60).

As per claim 10, Monier teaches said finite state machine includes a one-bit register indicating first and second step states (column 5, lines 47-55).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Monier (USP 5,764,554).

As per claim 1, Monier teaches a method for computing A^E modulo N, where A, E and N are integers, with $A < 2N$, all having binary representations, and where n is the number of bits in the binary representation of N (column 1, lines 40-44), and where $\Sigma = e, 2^i$, and where t is the number of bits in the binary representation of E, and where m and k are two positive integers such that mk = n (column 1, line 55), said method comprising the steps of:

providing a signal representing the constant, C, which is equal to 2^{+2mk} mod N (column 8, line 63) ;

multiplying said value A by said constant C using a circuit which accepts two input operands and which produces an output result value Zo given by A C 2^{-mk} modulo N (column 1, line 50 and column 7, line 30);

storing said value Zo in a first register and in a second register (column 7, line 64);

for sequential values of an index i running from 1 to t, repeatedly using the value in said second register as both of said operands for said circuit, with the output of said circuit being

stored back into said second register and, when e_{t-i}, is 1, using again the contents of said second register as one input operand to said circuit with said other input operand being said Zo value in said first register with the output of said circuit being stored in said first register (column 7, lines 54-62);

upon completion of said repetition, operating said circuit with the contents of said second register as one input operand with the constant 1 as said other input operand (column 7, lines 65-67); and

storing the output of said circuit in at least one of said registers , whereby said at least one register contains the binary representation of A^E modulo N (figure 3, element 108).

Monier is silent in disclosing that mk is greater than or equal to n+2. This modification would give them words of k bits ample storage space if the register were greater than n+2. One of ordinary skill in the art would know that a memory overflow would cause hardware to return invalid data.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Monier because it would allow the bits to be shifted without overflowing.

As per claim 1, Monier teaches a method for computing A^E modulo N, where A, E and N are integers, with $A < 2N$, all having binary representations, and where n is the number of bits in the binary representation of N (column 1, lines 40-44), and where $\Sigma = e, 2^i$, and where t is the number of bits in the binary representation of E, and where m and k are two positive integers such that mk = n (column 1, line 55), said method comprising the steps of:

providing a signal representing the constant, C, which is equal to 2^{+2mk} mod N (column 8, line 63);

multiplying said value A by said constant C using a circuit which accepts two input operands and which produces an output result value Zo given by A C 2^{-mk} modulo N (column 1, line 50 and column 7, line 30);

storing said value Zo in a first register (column 7, line 64);

if eo = 1, storing the value 1 in a second register, otherwise storing the contents of said first register in said second register (column 3, lines 60-63);

for sequential values of an index i running from 1 to t, repeatedly using the value in said second register as both of said operands for said circuit, with the output of said circuit being stored back into said second register and, when e_{t-i}, is 1, using again the contents of said second register as one input operand to said circuit with said other input operand being said Zo value in said first register with the output of said circuit being stored in said first register (column 7, lines 54-62);

upon completion of said repetition, operating said circuit with the contents of said second register as one input operand with the constant 1 as said other input operand (column 7, lines 65-67); and

storing the output of said circuit in at least one of said registers , whereby said at least one register contains the binary representation of AE modulo N (figure 3, element 108).

Monier is silent in disclosing that mk is greater than or equal to n+2. This modification would give the m words of k bits ample storage space if the register were greater than n+2. One

of ordinary skill in the art would know that a memory overflow would cause hardware to return invalid data.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Monier because it would allow the bits to be shifted without overflowing.

As per claim 4, Monier teaches final storing step stores the result in said second register (figure 3, element 108).

As per claim 5, Monier teaches a method for computing A^E modulo N, where A, E and N are integers, with $A < 2N$, all having binary representations, and where n is the number of bits in the binary representation of N (column 1, lines 40-44), and where $\Sigma = e, 2^i$ and where t is the number of bits in the binary representation of E, and where m and k are two positive integers such that mk = n (column 1, line 55), said method comprising the steps of:

repeatedly operating, for at most t cycles, a circuit which computes F G 2^{-mk} modulo N for binary input operands F and G to said circuit, with said circuit inputs being controllably selected, during each repetition, from the constant 1 , the constant 2^{+2mk} modulo N and the previous output from said circuit so as to produce an output of $A^E 2^{+2mk}$ modulo N (column 7, lines 54-62);

operating said circuit with one input being the output from said repeated step and the other input being the constant 1 , whereby the output of said circuit, after at most t cycles, is A^E modulo N (column 16, lines 53-57 and column 1, lines 59-60).

Monier is silent in disclosing that mk is greater than or equal to n+2. This modification would give the m words of k bits ample storage space if the register were greater than n+2. One

of ordinary skill in the art would know that a memory overflow would cause hardware to return invalid data.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Monier because it would allow the bits to be shifted without overflowing.

Conclusion

9. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
January 6, 2005

EMMANUEL L. MOISE
PRIMARY EXAMINER